National Infrastructure Protection Center
CyberNotes

Issue #21-99 *October 13, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified September 25, and October 7, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire (Windows NT[1]) ***A ColdFusion Serverpatch has been made available.[2]***	**ColdFusion**	**ColdFusion Server includes several undocumented CFML tags and functions that are used in the ColdFusion Administrator. As a result, developers who have permission to create Web applications and executable ColdFusion templates on a ColdFusion server can make use of the undocumented functions and tags to potentially gain unauthorized access to administrative settings including registry, database and advanced security settings.**	**No patch or workaround available at time of publishing.** ***ColdFusion Serverpatch has been made available at the Allaire Security Zone:*** http://www.allaire.com/security	**CFML Tag Vulnerability**	**High**	**Bug discussed in newsgroups and websites.**
FreeBSD[3] ***A fix has been issued.[4]***	**FreeBSD 3.0, 3.1, 3.2**	**A vulnerability exists in the new VFS cache introduced in version 3.0 which allows a local and possibly remote user to force usage of a large quantity of memory creating a Denial of Service condition.**	**No workaround or patch available at time of publishing.** ***Upgrade to the latest version of FreeBSD 3.3-STABLE to fix the problem.***	**VFS_Cache Denial of Service Vulnerability**	**Low**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Hybrid Network[5]	Hybrid Network's Cable Modems	Vulnerability exists in HSMP, which allows it to be reconfigured anonymously by a remote attacker. HSMP can also be used to configure the DNS servers used by cable modem users, allowing attackers to redirect cable modem subscribers to a Trojan site.	Cable providers should block out HSMP traffic (7777/udp) on their firewalls.	Cable Modem Remote Configuration Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM[6]	AIX 4.1.5, 4.2.1	Vulnerability exists in the 'named-xfer' executable, which allows members of the system group to overwrite any file in the system and gain root access.	Turn off the setuid bit on named-xfer. It is not required for its proper functioning.	Named-xfer File Overwrite Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[1] NTBugtraq, July 30, 1999.
[2] Allaire Security Bulletin (ASB99-10), September 29, 1999.
[3] Bugtraq, September 21, 1999.
[4] SecurityFocus, September 25, 1999.
[5] SecurityFocus, October 5, 1999.
[6] Bugtraq, September 23, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[7]	AIX 4.3.x	The ftpd daemon contains a buffer overflow vulnerability, which allows remote attackers to gain root access.	IBM is working on an official fix. A temporary fix, which has not been fully regression tested, is available via anonymous ftp from: ftp://aix.software.ibm.com/aix/efixes/security/ftpd.tar.z	AIX FTPD Remote Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Lee McLoughlin Mirror[8]	Mirror 2.9	Vulnerability exists in the Mirror Perl script, which allows remote FTP server operators to create or overwrite arbitrary files in the local system.	No workaround or patch available at time of publishing.	Mirror File Creation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Linux[9]	Linux	There is a buffer overflow vulnerability in cdda2cdr, which is distributed with the Cdwtools-0.93-78 package which allows a malicious user to r/w access to any hard drive(s).	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[10]	Linux Kernel 2.2.x	A weakness within the TCP stack in Linux 2.2.x kernels exists which make it possible to "blind-spoof" TCP connections. An attacker could initiate a TCP connection from an arbitrary non existing or unresponding IP source address, exploiting IP address-based access control mechanisms.	This vulnerability has been fixed in kernels 2.2.13pre13 and later. A patch is being proposed for earlier kernels.	ISN Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[11]	Mandrake 6.0	The GNOME libraries shipped with Mandrake Linux 6 contain a buffer overflow vulnerability that could allow an unauthorized user root access.	The fixed package is available at: http://www.linux-mandrake.com/en/fupdates.php3 or launch MandrakeUpdate.	GNOME Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published

[7] CIAC Information Bulletin J-072, September 30, 1999.
[8] SecurityFocus, September 30, 1999.
[9] Bugtraq, September 30, 1999.
[10] TESO Security Advisory,, September 26, 1999.
[11] Bugtraq, September 23, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[12] ***Microsoft has re-released Microsoft Security Bulletin.***[13]	**Microsoft Internet Information Server (IIS) 4.0; NT 4.0; BackOffice 4.5**	**IIS 4.0 allows an administrator the option to restrict access by specifying a domain or an IP address. Due to a regression error, a user who accesses an FTP site via a browser will be able to download files even if the files are marked "no access." The second problem is that IIS will allow access if it is unable to resolve the IP address of the requestor. This will occur even if the domain of the requestor has been restricted from access. This error only occurs on the first request.** ***The purpose of the re-release is to discuss an additional product, Microsoft Commercial Internet System, that is affected by this vulnerability.***	**A patch has been released that eliminates two vulnerabilities in IIS 4.0.** **Patch available at:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/** ***The information regarding IIS has not changed, and customers who previously applied this patch to their IIS systems do not need to take any action.*** ***IIS 4.0:*** ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/ ***MCIS 2.5:*** ftp://ftp.microsoft.com/bussys/mcis/mcis-public/fixes/usa/mcis25/security/ftpsvc-fix/	**IIS 4.0 Domain Resolution Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Microsoft Windows 95, 98, 2000, NT[14] ***Microsoft has released a patch for this vulnerability.***[15]	**Internet Explorer 5.0 for Windows 95, 98, 2000, NT 4.0**	**Vulnerability exists in IE5 that could allow a malicious web site operator to execute arbitrary programs on a victim's machine.**	**Until a patch is available, disable active scripting.** ***Microsoft has completed a patch that completely eliminates this vulnerability, which is available at:*** ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa	**Import Export Favorites Vulnerability**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[12] Microsoft Security Bulletin (MS99-039), September 23, 1999.
[13] Microsoft Security Bulletin (MS99-039), September 30, 1999.
[14] Microsoft Security Bulletin (MS99-037), September 10, 1999.
[15] Microsoft Security Bulletin (MS99-037, re-released September 24, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95, 98, NT 4.0[16]	Microsoft Internet Explorer 5.0	Security hole exists in Internet Explorer 5.0 that could allow a website to read a file on the computer of a user visiting the site. This security hole also extends to reading files on other computers connected to the visitors Local Area Network and Intranet.	The patch is available for download at either of the following Locations: http://windowsupdate.microsoft.com or, http://www.microsoft.com/msdownload/iebuild/dlbhav/en/dlbhav.htm	Download Behavior Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Microsoft Windows 95, 98, NT 4.0[17]	TeamShare TeamTrack 3.0	A vulnerability exists in the web server that is used to access the database, which allows unrestricted retrieval of any file on the filesystem.	TeamTrack also includes the option to use Netscape FastTrack/Enterprise or IIS instead. Change to one of these options.	Directory Traversal Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published
Microsoft Windows 95, NT[18]	Sambar 4.2.1	A Denial of Service vulnerability exists in the latest version of Sambar Web Server that causes the web server to crash without reporting any problem to the log file.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows 95/98/NT[19]	Internet Explorer 4.0; MSN Messenger Service 1.0; Known affected controls: Acrobat Control for ActiveX; Setupctl 1.0 Type Library; EYEDOG OLE Control module; MSN ActiveX Setup BBS Control; hhopen OLE Control Module; RegWizCtrl 1.0 Type Library	Several ActiveX applications contain buffer overflows. These buffer overflows can be used to execute arbitrary code on users' machines that have these ActiveX controls, just by passing a special argument to the ActiveX control (from a regular HTML page). Because these controls are marked as safe for scripting, they may be exploited through Internet Explorer, a web page, e-mail, or anywhere else where 'safe' ActiveX controls may be scripted.	Microsoft has released a patch to revoke the hhopen, regwiz and setupctl controls, and a previous patch has been released for Eyedog. For the other controls, and any others found to be vulnerable, see Microsoft knowledge base article Q240797 on how to stop an ActiveX control from running in IE. How to Stop an ActiveX Control from Running in Internet Explorer http://support.microsoft.com/support/kb/articles/q240/7/97.asp **Patch available at:** Internet Explorer 4.01 for Intel: ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE401/ImportExportFavorites-fix/x86/q241361.exe Internet Explorer 4.01 for Alpha: ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE401/ImportExportFavorites-fix/Alpha/q241361.exe Internet Explorer 5 for Intel: ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE50/ImportExportFavorites-fix/x86/q241361.exe Internet Explorer 5 for Alpha: ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE50/ImportExportFavorites-fix/Alpha/q241361.exe	ActiveX Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[16] Microsoft Security Bulletin (MS99-040), September 28, 1999; updated October 8, 1999.
[17] SecurityFocus, October 2, 1999.
[18] Bugtraq, October 4, 1999.
[19] SecurityFocus, September 27, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 9X/NT[20]	MacroMedia software - The Matrix Screensaver	"The Matrix" screensaver fails to require a password in all cases where it should. Even after setting the "Password protected" screensaver option, pressing the "Escape" keyboard key terminates the screen saver without the need for a password.	No workaround or patch available at time of publishing.	The Matrix Screensaver Password Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows NT[21] ***Microsoft has released patch for this vulnerability.[22]***	**Microsoft Windows NT 4.0, 4.0SP1, 4.0SP2, 4.0SP3, 4.0SP4, 4.0SP5**	**An unprivileged network user may gain admin privileges.**	**No workaround or patch available at time of publishing. Unofficial workaround: Enable Auditing on the HKEY_Local_Machine/SYSTEM/CurrentControlSet/Services/RASMAN key. Look for changes in the ImagePath value.** ***Hotfix available at:*** ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP6/Security/Rasman-fix/	**Privilege Escalation Vulnerability**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
Microsoft Windows NT 4.0[23]	Mediahouse Statistics Server versions 4.28 and 5.01	Server versions 4.28 & 5.0 contain security flaws in the web interface for remote administration of the Statistics Server. This vulnerability allows remote users to crash the server and possibly execute arbitrary code.	No workaround or patch available at time of publishing. Unofficial workaround is to remove read access from ss.cfg for Everyone/Authenticated Users, and block traffic to Port 80 of this system on an upstream router, if available.	Unchecked Buffer and Cleartext Password Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[20] Bugtraq, October 5, 1999.
[21] SecurityFocus. September 17, 1999.
[22] Microsoft Security Bulletin (MS99-041), October 1, 1999.
[23] Bugtraq, September 30,1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT, 95, 98[24] ***Exploit for this vulnerability has been published.***[25] ***Office 2000 is also contains this vulnerability.***[26] ***Microsoft has re-released this patch.***[27]	**Jet 3.51 driver (ODBCJT32. DLL) shipped with the Office 97 software suite** ***Office 2000 suite, Access 2000, Excel 2000***	**Vulnerability in Microsoft Office 97 can allow malicious code hidden in a web page or sent in e-mail to take control of online computers without the victims' knowledge. This vulnerability was first reported in Excel 97 but other Office applications can be used to hide the code.** ***Microsoft has released an updated patch that eliminates security vulnerabilities in the Microsoft(r) Jet database engine. A patch originally was released in August 1999, but an additional variant of one vulnerability, the "Text I-ISAM" vulnerability, was subsequently discovered. The new variant could allow a database query to delete files on a user's computer. This bulletin has been re-released to discuss the vulnerabilities in their entirety.***	**Upgrade to Jet 4.0 driver. This driver is delivered as part of MDAC 2.1 which can be downloaded at: http://www.microsoft.com/data/** ***Additional information and frequently asked questions regarding this vulnerability can be found at:*** http://www.microsoft.com/security/bulletins/MS99-030faq.asp ***Patch available at:*** http://officeupdate.microsoft.com/articles/mdac_typ.htm ***Newest Patch Available at:*** http://officeupdate.microsoft.com/articles/mdac_typ.htm	**MS Office Driver Vulnerability**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit has been published.*** ***Vulnerability has also appeared in the Press.***
QMS CrownNet Unix utilities for 2060[28] ***Update to QMS 2060 Printer Password Vulnerability***[29]	**QMS 2060 Network Printer**	**Root access to the printer can be gained without root's password. By gaining this access privilege, any attacker can gain full control of the printer.**	**No workaround or patch available at time of publishing.** ***After a lengthy investigation with QMS customer support it became apparent that this is not a bug but a feature. In order to make root password protected one has to buy a security key, which is a DB-9 plug, which is plugged, in the matching connector at the rear of the printer.***	**Printer Password Root Vulnerability**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[24] Bugtraq, July 29, 1999.
[25] NTBugtraq, August 11, 1999.
[26] Microsoft Security Bulletin (MS99-030), August 20, 1999.
[27] Microsoft Security Bulletin (MS99-030), October 8, 1999.
[28] NTBugtraq, August 18, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Red Hat[30]	Red Hat 6.0	A vulnerability exists in the rpmmail package distributed with the Extra Applications CD, which could lead to unauthorized remote or local root access.	No workaround or patch available at time of publishing. Unofficial workaround is to disable rpmmail (remove it from your /etc/aliases file) until further notice.	RPMMail Security Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SCO[31]	UnixWare 7.1	A vulnerability exists in UnixWare's DOS Utilities Package, which allows users who are able to execute the program the ability to gain root privileges.	No workaround or patch available at time of publishing.	DOS Utilities Package Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun[32] ***Exploit script has been published.***[33]	**Solaris 2.6_x86, 2.6**	**A vulnerability in Solaris TCP/IP stack may allow remote users to panic the system.**	**For Solaris 2.6 sparc apply patch 105529-07. For Solaris 2.6 x86 apply patch 105530. ftp://sunsolve.Sun.COM/pub/patches/Solaris2.6_x86.PatchReport**	**Recursive Mutex_enter Panic Vulnerability**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Sun[34] ***Sun releases more patches***[35]	**Solaris 2.6_x86, 2.6, 2.5.1_x86, 2.5.1**	**The dynamic linker ld.so.1 contains a vulnerability when profiling dynamic libraries, which allows a malicious user to create world writeable files as root anywhere in the file system.**	**Solaris patches available from http://access1.sun.com Solaris 2.5.1 103627 Solaris 2.5.1x86 103628 Solaris 2.6 105490 Solaris 2.6x86 105491** ***It's been fixed in Solaris 7 and with the following patches in other releases: 103242-07: SunOS 5.5: linker patch 103243-07: SunOS 5.5_x86: linker patch***	**LD_Profile Vulnerability**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
SuSE Linux[36]	Linux distributions using mirror version 2.8.f4 and earlier	A vulnerability in the mirror package exists that could allow a malicious user to create directories, enabling the creation of files one level above the local target directory for the mirrored files.	Update the mirror package: http://www.suse.de/patches/index.html	Mirror Package Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[29] Bugtraq, September 24, 1999.
[30] Bugtraq, October 5, 1999.
[31] Bugtraq, October 5,1999.
[32] SecurityFocus, September 24, 1999.
[33] SecurityFocus, September 24, 1999.
[34] SecurityFocus, September 22, 1999.
[35] Securiteam, September 24, 1999.
[36] SuSE Security Announcement, October 1, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[37]	Cactus Software's shell-lock	A vulnerability exists in the shell-locked binary, which can lead to root access.	No workaround or patch available at time of publishing.	Shell Lock Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[38]	Knox Software's Arkiea Backup Package	A local buffer overflow in the handling of the HOME environment variable by the rlserver and rnavc binaries allows local users to obtain root access.	No workaround or patch available at time of publishing. Unofficial workaround is to turn off the setuid bits from the rnavc and nlservd executables.	Arkiea Backup Rnavc & Nrserverd HOME Environment Variable Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[39]	Omni-NFS/X Enterprise 6.1	A vulnerability exists in the nfs daemon (nfsd.exe), which allows remote attackers to cause a Denial of Service attack.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[40] ***Exploit script has been published.[41]***	**Solaris 2.7**	**A possible buffer overflow vulnerability exists in the sgid mail/usr/bin/mail, which allows execution of any command a malicious user wants.**	**No workaround or patch available at time of publishing.**	**Usr/bin/mail Security Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Unix[42]	SSH Communi-cations Security SSH 1.2.27	A vulnerability in SCI's creation of the authentication agent Unix domain socket allows local users to create a Unix domain socket with an arbitrary file name in the system.	No workaround or patch available at time of publishing.	SSH Authentication Socket File Creation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[37] L0pht Security Advisory, October 4, 1999.
[38] Bugtraq, September 23, 1999.
[39] Bugtraq, October 6, 1999.
[40] Securiteam, September 16, 1999.
[41] Bugtraq, September 27, 1999.
[42] Securiteam, September 20, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix/Windows 95/98/NT. [43]	Inline Internet Systems Inc.'s iHTML Merchant	Vulnerability in iHTML Merchant allows a malicious hacker to view the protected files in the website's administrative section, giving the attacker the ability to view credit card information. If the iHTML Merchant is being run on Windows 95/98/NT the vulnerability is much more severe. If the iHTML Merchant is being run on UNIX, it is possible to alter the web site content.	Inline Internet Systems has released patches for the "feedback vulnerability" in iHTML Merchant. Available at: http://www.ihtmlmerchant.com/support_patches_feedback.htm	IHTML Feedback Vulnerability	**High**	Bug discussed in newsgroups and websites.
Yahoo[44]	Yahoo Instant Messenger Build 733, 734	A Denial of Service vulnerability exists in Messenger Build 733 and 734.	Patch Locations (new build): http://rd.yahoo.com/pager/zd/?http://download.yahoo.com/dl/ymsgr.exe	Messenger remote Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[43] Team Asylum Security Advisory, September 28, 1999.
[44] Bugtraq, September 28, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between September 25 and October 7, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 50 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
October 7, 1999	**Hybrid_network_cable_modems.txt**	**Exploit script that allows remote attackers to anonymously reconfigure any Hybrid Network's cable modem running HSMP.**	
October 7, 1999	Inews.c	Buffer overflow in inews, which gives egid inews.	
October 6, 1999	**Cdda2x.sh**	**Shell script, which exploits the Linux x86 cdda2cdr vulnerability.**	
October 6, 1999	**Omni-NFS_DoS.txt**	**A Denial of Service exploit against the the nfs daemon (nfsd.exe) used by Omni-NFS/X.**	
October 6, 1999	**SCO_root_exploit.txt**	**Root exploit for the SCO UnixWare /usr/lib/merge/dos7utils program vulnerability.**	
October 6, 1999	Vetescan10-06-1999.tar.gz	Vetescan is a bulk vulnerability scanner.	
October 6, 1999	Vetetcl.tar.gz	TCL version of Vetescan for use with eggdrop.	
October 5, 1999	**Cdda2cdr_bof.txt**	**A root compromise exploit script for the buffer overflow vulnerability in the cdda2cdr cdwtools-0.93.78 package.**	
October 5, 1999	**l0pht.99-10-04.shell-lock.txt**	**Exploit script for the shell lock vulnerability.**	
October 5, 1999	**RH6_rpmmail_exploit.txt**	**Root exploit for the rpmmail vulnerability in Red Hat 6.0.**	
October 5, 1999	**Sambar_D0S.txt**	**A Denial of Service attack script against the Sambar HTTP_Server 4.2.1 running on Windows 95.**	
October 4, 1999	Downgrade.exe	Fake SMB server that tries a dialect downgrade to get plaintext passwords from remote users for Windows NT.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
October 4, 1999	Inzider.exe	Shows which processes listen at which ports, and can be used to find Back Orifice 2000 when it is hidden in another process. For Windows 9x/NT.	
October 4, 1999	Winfo.exe	Uses Null Sessions to retrieve account and share information from Windows NT.	
September 30, 1999	**Aix-ftpd.pl**	**Remote buffer overflow exploit script against AIX's ftpd.**	
September 28, 1999	Bindinfo.c	Bindinfo v1.01 allows root to make DNS queries behind firewalls. Works on Solaris and OpenBSD.	
September 28, 1999	Guilecool	Scans for 44 known vulnerabilities.	
September 28, 1999	Guile-scan.c	CGI Scan v3.1 scans for vulnerable web servers.	
September 28, 1999	Leapfrom_1_0a.tar.gz	Leapfrog 1.0 will redirect any port. It can be used to work around firewall configuration and other issues requiring a port redirect.	
September 27, 1999	ActiveX_bof.txt	Several ActiveX buffer overflow exploit scripts..	
September 27, 1999	**Adv1.tar.gz**	**Exploit script that allows remote users to guess the initial sequence number of TCP sessions.**	
September 27, 1999	**Cfingerd_bof.txt**	**Xfingerd version 1.4.2 local buffer overflow exploit script.**	
September 27, 1999	**Dtaction.digital.unix.vuln.txt**	**Local root exploit against the dtaction vulnerability in CDE.**	
September 27, 1999	FreeBSD-SA-99.05.fts.txt	FTS library routine vulnerability exploit script.	
September 27, 1999	Hhopen.txt	Microsoft hhopen OLE control buffer overflow vulnerability script.	
September 27, 1999	Linux_GNOME_exploit.txt	Virtually any program using the GNOME Libraries are vulnerable to a buffer overflow attack.	
September 27, 1999	Lynx.2.8.2.extern.txt	Exploit script that can be used against lynx to activate commandline parameters.	
September 27, 1999	Regwizc.txt	Microsoft IE Registration Wizard Buffer Overflow vulnerability script.	
September 27, 1999	**Sco_local_exploit.txt**	**SCO 5.0.x exploits for scosession and scoterm allowing bin/root respectively.**	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
September 27, 1999	SDI.exploit4.proftpd.txt	Root exploit for the ProFTPD log_xfer buffer overflow vulnerability.	
September 27, 1999	Setupbbs.txt	Exploit script for Microsoft's MSN Setup BBS ActiveX Control Buffer Overflow Vulnerability.	
September 27, 1999	Setupctl.txt	Exploit script for Microsoft IE Setupctl ActiveX Control Buffer Overflow Vulnerability.	
September 27, 1999	Solaris_root_exploit.txt	Local root exploit for Solaris 2.6 and the way it handles $LD_PROFILE.	
September 27, 1999	**Solaris_x86_mail_exploit.txt**	**Working Solaris x86 /usr/bin/mail exploit.**	
September 27, 1999	**Solx86gid.c**	**Generic Solaris x86 exploit script for use against sgid binary.**	
September 27, 1999	**SSH.1.2.27.DOS.txt**	**Exploit script for SSH "authentication sockets", used to pass authentication keys securely.**	
September 27, 1999	**Ssh_exploit.txt**	**Exploit script for SSH "authentication sockets", used to pass authentication keys securely.**	
September 27, 1999	**SuSE_overflow_exploit.txt**	**Local root exploit for Linux x86 /usr/bin/sccw vulnerability.**	
September 27, 1999	**SuSE_root_exploit.txt**	**Local root exploit for Linux x86.**	
September 27, 1999	Suse6.2pbpg.txt	Exploit script for SuSE 6.2, which allows any user to read any file on the system.	
September 27, 1999	**Unix_virus.c**	**A fully functional Unix virus that will infect your manpages when started.**	
September 27, 1999	Unsetenv.txt	Exploit script for use against the unsetenv function in glibc 2.1.1.	
September 26, 1999	**Knox.c**	**Local root exploit script for Linux x86 Arkiea nlserverd buffer overflow vulnerability.**	
September 26, 1999	**Sccwx.c**	**Local root exploit script for Linux x 86 on SuSE 6.2.**	
September 24, 1999	Autfp25.tgz	A buffer overflow exploit script for wuftpd.	
September 24, 1999	Kbd.c	Linux loadable kernel module backdoor for 2.0.x which allows root access by modifying the SYS_creat and SYS_getuid system calls.	
September 24, 1999	ShadowNWCrack.zip	Code for breaking Novel NetWare 4.x.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
September 24, 1999	Soltera.c	Exploit script for Sun's mutex_enter vulnerability that causes the system to panic.	
September 24, 1999	Superscan.zip	A windows based port scanner which is multi-threaded and has no TCP/Stack memory problems.	
September 23, 1999	Gnox.sh	Generic exploit for GNOME applications uncer Linux x86.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

- Analysis indicates that Hostile Active Code is now the hacker's weapon of choice.
- HTTP Unix Password attacks and HTTP Test_CGI attacks have occurred lately.
- Web hacks using Cold fusion vulnerabilities continues.
- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP port 3128.
- Weak passwords continue to be the number one cause of system compromise.
- A recently publicized vulnerability is being used to modify web pages and turn off logging.
- Infrastructure attacks continue to be directed against corporate e-mail systems.

Viruses/

W32/Pretty.Worm: This is a worm that infects Windows 9x/NT files. When run this program will display a "3D Pipe" screen saver and then will copy itself to files32.vxd in Windows/System folder. It then modifies the registry key value "command" located in the location:

HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open

From "%1"%" to FILES32.VXD "%1"%". This will cause the FILES32.VXD to run during the execution of any exe file.

This worm will try to e-mail itself automatically every 30 minutes to all e-mail addresses listed in the Internet address book, it will also try to connect to an IRC server and join a specific IRC channel. While connected to the IRC server it is possible for an unauthorized user to execute commands and obtain information, such as the computer name, registered owner, registered organization, system root path, and Dial Up Networking username and passwords.

VBS_FREELINK: VBS/Freelink is written in the VBScript language. By default, programs written in VBScript operate only under Windows 98 and Windows 2000 beta (unless Windows Scripting Host has been installed separately). However, Microsoft Internet Explorer 5 installs Windows Scripting Host (WSH) on Windows 95 and Windows NT 4.0 machines by default, making them vulnerable to this worm.

The worm arrives to users in e-mail message attachments named LINKS.VBS (this is the default name and may be changed). When it is executed, the worm shows a message box with the following text:

> This will add a shortcut to free XXX links on your desktop. Do you want to continue?

Whether the user clicks 'yes' or 'no', the program creates an Internet shortcut named "FREE XXX LINKS" to the desktop. This shortcut points to a porn web site. After this, the worm searches for mapped network shares on the local network. If the worm finds any network drives, it copies itself to the root of them.

The worm uses Outlook application to mass-mail itself to each recipient in each address book. The mass-mail portion is similar to the Melissa virus.

W97M_Michael.KBD: This is a destructive macro virus that has been found in the wild in Asia. It re-maps the keyboard and deletes all user macros before it infects Word 97 files. When an infected user clicks on the Print icon, the virus checks the current date and month. If the current date is greater than 23 and the current day is a Friday, the virus dumps a file "dummy.txt" which most likely contains a fake resume of the creator, in c:\Windows. After which the virus prints this file.

If an infected user saves a file, the virus checks if the current date of the month is greater than 23 and the current day is equal to Saturday. If it is, it displays this message in the status bar:

> Michael Learns to Hack

And then it displays another message:

> And Hope You'll Learn From It Too

If an user opens a file, the virus checks if the current date of the month is equal to 30 and if it is, the virus displays a balloon with the creator's information together with the quotations listed above displayed randomly.

Dmsetup (October 3, 1999): This is the most common name associated with a worm that attempts a number of different actions. The actions include coping itself into multiple directories, mailing itself to other users, modifying the autoexec.bat and config.sys files, modifying an number of irc files, and creating multiple folders on the infected system.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #99-20 and will be added on a cumulative basis. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Backdoor	0.1	Current
Bobo		CyberNotes 99-20
BrainSpy	Beta	Current
Deepthroat	3.1	CyberNotes 99-20
Doly	1.1-1.6	CyberNotes 99-20
Donald Dick	1.52	CyberNotes 99-20
Eclipse 2000		CyberNotes 99-20
InCommand	1.0	CyberNotes 99-20
Ini Killer	2.0-3.0	Current
Irc3		Current
Logger		Current
Matrix	1.4-1.5	CyberNotes 99-20
Millennium	1.0-2.0	Current
NetSphere	1.0-1.31337	CyberNotes 99-20
SubSeven	1.0-2.0	Current
WarTrojan	1.0-2.0	Current
Xplorer	1.20	Current
Y2K Countdown (Polyglot)		CyberNotes 99-20

War Trojan v1.0 and 2.0 (October 3, 1999): War Trojan has many features of NetBus, with a few extra, including; e-mail bomber, TCP/UDP flooder, and e-mail spoofer. This Trojan also changes Internet Explorers start-page to a URL voting page.

Backdoor v.0.1 (September 29, 1999) Backdoor is a Trojan, which is distributed as two files. One file is a readme.exe and the other is icqnuke.exe, which fakes an icq nuke app. Each of these is a part of the Trojan and although the Trojan will work after just one is run, both are needed for full effects. One of the good things about this Trojan is that is requires certain DLLs to already be present, or installed along with the Trojan. These DLLs are needed for both the Trojan and the client as well.

Inikiller v2.0 (September 29, 1999): Basic Trojan with a few destructive commands. Can easily destroy data on your system.

Millenium v2.0 (September 29, 1999): Millenium is a Trojan, which is very similar to BackOrifice, however has a much nicer GUI even compared to NetBus. One major difference is that Millenium is more difficult to detect and remove.

Brainspy Beta (September 27, 1999): Another basic Trojan with many NetBus features.

IRC3 (September 27, 1999): This Trojan installs an FTP server that allows access to your whole harddrive. Fortunately removal is easy and painless.

Xplorer 1.20 (September 27, 1999): This Trojan has a few features of NetBus (and more to be planned for later releases), however its main feature is that there is no custom windows GUI client. All Trojan control is done through telnet, which makes an infected system hackable from not only other windows systems, but Unix and Mac as well.

Subseven 1.4 added (September 27, 1999): The SubSeven Trojan has the exact same feature list as NetBus, with one original feature: The server can send the hacker your IP when you connect to the internet by either e-mail AND/OR icq.

Logger (October 3, 1999): Logger is a basic keylogger, which stores all keypresses made on your system to a file that may be retrieved by an unauthorized user. It also features a 'real time' key monitor that allows an Internet user can watch what you type, as you type it.